4. Application of Neural Networks to Power System Security Assessment and Enhancement

R. Fischl
Electrical and Computer Engineering Department
Drexel University
Philadelphia, PA 19104, USA

Dagmar Niebur
Jet Propulsion Laboratory,
California Institute of Technology
Pasadena, CA 91109, USA

M. A. El-Sharkawi
Department of Electrical Engineering
University of Washington
Seattle, WA 98195, USA

Abstract - This tutorial presents an overview of the application of artificial neural network (ANN) to power system security assessment (SA) and security enhancement (SE). The main objective of this tutorial is: (i) to identify the type of security problems best suited for ANN application and (ii) to give a procedure for designing ANNs for SA and SE, specifically, how to choose a good ANN; the inputs, the training set and how to evaluate the ANN performance. Since the SA assessment problem involves classification, pattern recognition, prediction, estimation, and fast solution, it is well suited for ANN application. The majority of ANN architectures used in SA and SE are the multi-layered perceptron, the Kohonen and the Hopfield networks. The problem of selecting a good ANN for SA and SE is similar to the problem of selecting a set of good security indices or approximate system performance (ASP) models, i.e. the representation problem in Approximation Theory. Although the key issue in the selection of a good ASP model is that it be computationally fast, this is a non-issue when using ANN's. On the other hand the accuracy of the prediction of the security level is of paramount importance since explicit expression of the input-output map of the ANN is not available for evaluation and, in addition it is adaptive. To help address this issue, this tutorial also gives a method for evaluating the ANN design in terms of its accuracy in predicting the correct level of security. Various examples are given to give the reader an insights into the specifics of problems relating to the design of ANN for SA and SE. An extensive literature list points the reader to more detailed information.

1. INTRODUCTION

Power system security assessment is the process of determining whether the power system is in a secure or alert (insecure) state, where secure state implies that the load is satisfied and no limit violations will occur under present operating conditions and in the presence of unforeseen contingencies (i.e., outages of one or several lines, transformers or generators) [Balu *et al*., 1992]. The alert (or emergency) state implies that either some limits are violated and/or the load demand cannot be met and corrective actions must be taken in order to bring the power system back to the secure state. The key issues in security assessment are: (i) fast identification of the set of insecure contingencies; and (ii) their evaluation in terms of the severity of their impact on the power system operation (i.e., contingency ranking). The solution Of these problems involves prediction, pattern recognition, classification and fast solution, which are tasks well suited for the ANN technology.

Over the past few years, a number of approaches using artificial neural networks (ANNs) have been proposed as alternative methods for security assessment in power system operations [Mori and Tsuzuki, 1990, El-Sharkawi *et al.*, 1992, CIGRE TF 38.06.06, 1993, Germond and Niebur, 1993; IEEE TF, 1995; Dillon and Niebur (ed.), 1995]. In general, ANN methodology should be applied in areas where conventional techniques have not achieved the desired speed and accuracy. One such area is the fast pattern recognition and classification of the system security status in the area of contingency analysis. This application is possible because an ANN can be trained to acquire knowledge of the complex relationships between the initial system state and the post-contingency state in a power system through the use of an iterative mathematical algorithm. Once properly trained, a ANN can interpolate patterns using a limited amount of input data [Fischl and Chow, 1993]. Since ANNs are quick in response time and can be easily adapted, they become excellent candidates for on-line application in areas where inadequate input data and computational burden might have rendered other approaches impractical for implementation.

There are a number of problems with using the ANN to assess the power system security. For a multi-layered perceptron (MLP), there is no exact criterion for the number of hidden layers as well as the number of neurons per hidden layer. Too many neurons can lead to memorization of the training data with the danger of losing its ability to generalize and predict. Another problem is the selection of the training set. Considering that ANNs are good in interpolation but not in extrapolation, training sets have to be representative of the different states of the power system. This means that they need to comprise of the complete pattern space of the secure and insecure power system operation. This means a large training set, which implies a long time for training. Furthermore, there is the problem with data sensitivity, as there is no fixed rule as to what type of input data would provide the best results in the output.

Finally, most ANN design procedures (supervised or unsupervised) are based on a procedure which optimizes the ANN weights with respect to the approximation error of neuron output and target output, usually the security state, (e.g., the back propagation (BP) method minimizes a mean-square-error). However ANN design procedures should focus on the maximization of the accuracy of the security prediction especially in the critical and insecure areas of the power system operating space by taking the probability and severity of the security states into account.

Table 1 gives a comparison between the conventional and neural computation of power system security. In the next section we shall address the issues presented in this table, concerning the design of the ANN. Before, doing this we give more details relating the items in the *Conventional computation* column of Table 1.

Table I: Comparison of Conventional and Neural Computation of Power System Security

Task	Conventional computation	Neural network computation
Security Assessment & Enhancement	Selection of Approximate System Performance (APS) model & Algorithm	Selection of Neural Network Architecture & processing rule
Input data	Data from State Estimator: Network data; Injections; Contingency List & Operating constraints (Numerical form only)	Processed injection & network data to reduce the input data set plus operator data (Both numerical & perceptual data)
Knowledge acquisition	Programming	Weight determination, i.e., training set & learning rule
Knowledge retrieval	Sequential computation	Fast parallel computation
Computation	High-precision arithmetic to determine if ASP model predicts limit violation or	Low-precision, nonlinear mapping to predict the level of insecurity; or a low precision contingency filter
Stored parameters	ASP model parameters are estimated & held constant	Values of weights are adapted via a learning rule

2. WHAT IS SECURITY ASSESSMENT AND ENHANCEMENT?

'A reliable power system should be operated so that it can withstand the outage of any system component or a set of components. To this end, most power systems are operated on rr first contingency basis. A contingency is a set of hypothetical network equipment outages or breaker operation such as the loss of a generator, transmission line, a transformer or a combination Of such. In contingency analysis, user-specified outages tire examined to assess the effect of contingencies and alert the system operators to the potentially harmful ones that violate the equipment operating limits and/or drive the system to voltage and phase angle instability or excessive frequency deviations. The most common limit violations includes transmission line and/or transformer thermal overloads, abnormal voltages and excessive voltage deviations. Given this information, a system operator can judge the relative severity of each contingency and decide if preventive actions should be initiated to mitigate the potential problems. The best control strategy fur moving the system from an insecure state into secure states is what is called security enhancement (SE).

The traditional contingency selection and ranking approach is to use some type of *automatic contingency selection* (ACS) or *contingency screening* (AS) method. In either case, the key to a good A('S or AS method is that it is fast in computation and accurate in correctly identifying the harmful contingencies, that is quickly reducing the contingency list by eliminating all the irrelevant (or harmless) contingencies. Moreover, it must rank the contingency in relative severity and if possible predict the post-contingent line flows, voltages, frequency and system stability. To achieve this, various algorithmic methods have been proposed, each of which uses an *approximate system performance* (AS]') model which are computationally efficient to either identify the insecure contingencies and/or estimate the enhancement strategy [Balu *et al.*, 1992, El-Sharkawi *et al.*, 1992]. The ASP model can be either a scalar performance index (i.e., security index), or a linearized system model (such a\ distribution factors), or a simplified dynamic model

The standard approach to the security assessment problem is to perform first the static security analysis and then the dynamic security analysis. The *static security analysis* evaluates the post contingent steady state of the system neglecting the transient behavior and any other time-dependent variations due to changes in load-generation conditions. On the other hand, the *dynamic security analysis evaluates* the time-dependent transition from the pre-contingent to the post-contingent state, specifically, the stability of the system both from the small and large perturbation point-of-views. Most of the present Energy Management Systems (EMS) perform only the static security analysis. The dynamic security analysis methods are not fully operational and are currently being tested and evaluated. In the following sections issues in static security assessment and dynamic security assessment will be discussed and three case studies of application of neural networks will be presented.

2.1. *Static Security Problem*

In static security analysis the power system is modeled by a set of equality constraints representing the power balance al each bus (called load flow equations) and a set Of inequality constraints representing the thermal, voltage and generator VAr limits. For a network with n busses, the load flow equations can be written in a general form as:

$$\text{Real Power} \qquad f_{pi} = P_i - P_i(\mathbf{x}, \mathbf{Y}, C_\lambda) = 0, \qquad i = 1, \ldots, n \tag{1a}$$

$$\text{Reactive Power.} \quad f_{qi} = Q_i - Q_i(\mathbf{x}, \mathbf{Y}, C_\lambda) = 0, \qquad i = 1, \ldots, n \tag{1b}$$

where P_i and Q_i denote the net real and reactive power injection at bus i, respectively; $P_i(\mathbf{x}, \mathbf{Y}, C_\lambda)$ and $Q_i(\mathbf{x}, \mathbf{Y}, C_\lambda)$ denote the real and reactive power consumption by the network which depend on the voltage vector $\mathbf{x} = [V_d^T, \theta^T]^T$; Y denotes the network parameters; and C_λ denotes the contingency Specifically:

$$P_i(\mathbf{x}, \mathbf{Y}, C_\lambda) + jQ_i(\mathbf{x}, \mathbf{Y}, C_\lambda) = E_i \sum [Y_{ij}(C_\lambda) E_j]^* \tag{2}$$

where $E_i = V_i / \theta_i$: complex voltage at bus i; Y_{ij} = the ij^{th} element of the bus admittance matrix.

For secure operation, the solution $\mathbf{x}$ of Eq. (1) must satisfy the thermal or line flow limits, reactive power limits, voltage limits and voltage drop limits, which can be represented in a general form by

$$z^L \le z(\mathbf{y}, C_\lambda) \le z^U \tag{3}$$

where the superscripts L and U denote the lower and upper limits and $z(\mathbf{y}, C_\lambda)$ denotes the line flows, load bus voltages and generator vars. The vector $\mathbf{y}$ in $z(\mathbf{y}, C_\lambda)$ emphasizes that each response variable z_j, depends on the injections $\mathbf{y}$ (which represents all the independent variables, namely, the real and reactive load bus powers, P_d and Q_d, generator P_g and voltage magnitude V_g) via the solution of Eq.(1).

Based on the above, the detection of insecure contingencies is a hypothesis testing problem which determines whether or not the constraints of (1) and (3) are satisfied for the present operating point, $\mathbf{y}$, and the set of postulated contingencies $\{C_\lambda, \lambda = 1, \ldots, N_c\}$, i.e.,

$$H_1 \text{ (Contingency insecure: at least one limit violation)}: (\mathbf{y}, C_\lambda) \notin SS \tag{4}$$

$$H_0 \text{ (Contingency secure: no limit violation)}: \qquad (\mathbf{y}, C_\lambda) \in SS$$

where SS is the set Of all $[\mathbf{y}, C_\lambda]$ satisfying Eqs. (1) and (3). Since both the power injections, $\mathbf{y}$, and contingencies, C_λ, are uncertain because of such disturbances as uncontrolled loads, weather, component outages, etc., the security assessment problem is probabilistic in nature.

To obtain an appraisal of the severity of each insecure contingency, there are basically two (?) approaches: either (i) a ranking index is used to evaluate the level of overload; or (ii) a set of discrete levels is used to determine the severity of the limit violations, that is:

$$z^{L_s} \le z(\mathbf{y}, C_\lambda) \le z^{U_s}, \; s = 1, \ldots, N_s \tag{5}$$

where superscripts L_s and U_s denote the lower and upper limit fur the severity level s; N_s denotes the number of severity levels at which appropriate corrective actions should be taken by system operators. In most cases, this type of coarse severity level information is sufficient for system operators to initiate preventive or corrective actions, and the exact post-contingency value is only of secondary importance.

In summary, the static security assessment problem implies solving Eq (4) for all postulated contingencies, where each contingency represents the outage of either one or a set of lines and/or generators. This implies the evaluation Of (4) for all combinations Of m failures out of n elements, which is an extremely large number. For large power networks, even a reduced set Of contingencies cannot be treated in real time and therefore various approximating models and methods have been developed. Some of these are discussed next

2.?. *Static Security Analysis: Conventional Techniques*

To reduce the computational effort Of the security assessment, presently, most Energy Management Systems (EMS) use one or more Security Assessment (SA) predictors (such as sensitivity matrix, distribution factors, fast decoupled load flows, or performance indicators) to reduce the number of critical contingencies to be calculated explicitly in real-time There are many SA predictors available, each making certain assumptions on the network or the operating states, in order to reduce the computation effort in the evaluation. For example, the simplest scalar SA predictors are of the scalar category having the general form [Fischl and Chow, 1993]:

$$PI(\mathbf{y}, C_\lambda) = \sum_k w_k h_k(\mathbf{y}, C_\lambda) \tag{6}$$

where PI stands for Performance Index; $h_k(\mathbf{y}, C_\lambda)$ is a real-valued function of $(\mathbf{y}, C_\lambda)$ and $\{w_k\}$ are positive weighting coefficients. The notation $PI(\mathbf{y}, C_\lambda)$ emphasizes that the PI is evaluated at the operating point, $\mathbf{y}$, and contingency, C_λ. This PI is used both for insecure contingency detection and severity ranking. The contingency classification is performed using the following criterion:

d_1 (Contingency insecure; at least one limit violation): $PI(u,C_\lambda) > TH$

d_0 (Contingency secure; no limit violation): $PI(u,C_\lambda) \leq TH$

where TH is some specified or calculated threshold value. This criterion is used for either thermal loading limit violation check, or voltage limit violation check, or voltage stability check when the PI in (7) represents either a loading index, or a voltage index, or a stability index, respectively.

Although this type of SA predictor is computationally efficient, it may not classify the contingencies correctly. The cumulative effect of the approximations made by the SA predictor and the uncertainties due to the exogenous factors (such as uncontrollable load and weather conditions) lead to two types of errors in security classification: *missed detection* and *false alarm*. A ***missed*** detection is one in which the assessment says that the system is secure, but in reality it is not. A false alarm is one in which the assessment says that the system is insecure. While in reality *no system constraints* have been violated. The two errors can be quantified using Eqs. (4) and (7), in terms of the probability of missed detection, P_{md}, and the probability of false alarm, P_{fa}, as follows:

$$P_{fa} = P_r\{d_1 \mid 11(,) \quad (8a)$$

$$P_{md} = P_r\{d_0 \mid 11]\} \quad (8b)$$

A good security assessment "predictor" is therefore one that has the least amount of false alarms and no missed detections [Fischl and Chow, 1993, Chow *et al.*, 1992]. Therefore Eq.(8) gives the performance index for evaluating any SA predictor, including a ANN-based SA predictor.

2.3. Application of ANN to Static Security Assessment

2.3.1. Type of ANN Architecture

2.3.1.1. Supervised Architectures

As seen in the references the most popular choice of NN is the multi-layered perceptron. The reason for this is its ability to learn on-line. The problem is the selection of the training set and the selection of the inputs. A good method for reducing these is to use some of the security indicators presently calculated by the EMS system as inputs to the ANN. This will make the ANN act as a post-processor for improving the accuracy of the security prediction.

In [El-Sharkawi *et al.*, 1990] one specific contingency is fixed in advance. The security boundaries are then trained with a MLP which is used as a decision tool in order to determine whether an unknown operating point lies inside the security boundaries of the space of injections with respect to this specific contingency.

The use of the Hopfield network was exploited in [Yan *et al.*, 1991] for the prediction of the class of violations for post-contingency bus voltages, voltage drops and line flows. The ANN is then used to determine the severity of the violation and the limiting contingency provoking this violation in the first place. The last step is formulated as a binary optimization problem. Only a subset of all contingencies is chosen for this application. The architecture of the Hopfield network is used as an associative memory for the retrieval of the limiting contingencies under certain assumptions. Instead of calculating the weights of the Hopfield net using the sum of outer products of the input vectors, the weights are determined using linear programming which guarantees a larger region of convergence [Fischl *et al.*, 1990].

Both MLP and Hopfield network therefore reduce the dimensionality of the problem by reducing the number of contingencies and often by keeping insignificant power variables constant.

2..?, 1.2. *Unsupervised and Hybrid Architectures*

Unsupervised networks either reduce the dimensionality of the security assessment problem by reducing the dimension of the operating vector or by quantizing the operating space. These techniques fall into the same category of techniques as statistical feature detection algorithms or clustering techniques.

For security assessment unsupervised networks often act as a data pre-processor for a contingency analysis tool or a neural network. The unsupervised layer is used for data reduction, the supervised layer for data retrieval, which usually includes the security class of the operating state. Examples are discussed in [Weerasooriya and El-Sharkawi, 1991] where the Karhunen-Loève Transformation is combined with a MLP, in [Sobajic *et al.*, 1990] where A}< 'J'-? like network is combined with the Functional-Link Net, or in [Ranaweera and Karady, 1993] where the Radial Basis Functions Network consisting of a Kohonen layer for quantization and a linear supervised layer.

in [Weerasooriya and El-Sharkawi, 1991] for reduction of the dimension of the input data vector is achieved with the principal component analysis method (also called Karhunen-Loéve expansion). This method determines the eigenvectors corresponding to the largest eigenvalues of the auto-correlation matrix of training vectors as its principal components. The reduced training vectors are selected in direction of the most dominant eigenvectors. Using this new set of reduced vectors, a MLP is then trained to identify the security boundaries of the operating space (see comments to reference [El-Sharkawi *et al.*, 1990] above.)

Quantization of the operating space into prototype operating states has been proposed for the security assessment of a small space station transmission system in [Sobajic *et al.*, 1990]. An unsupervised ART2-like ANN is used for the clustering of the input vectors. For this ANN each cluster has an adaptively determined center, the typical operating state, and a radius which has to be determined in advance, usually through experimentation. Feature retrieval, that is, the security state of each typical operating scenario is implemented in a supervised manner with the Functional Link Net architecture.

A different quantization approach for identifying the security region is the self-organizing feature map presented in [Niebur and Germond, 1991] and [El Sharkawi and Atteri, 1993]. Each neuron has one weight vector which represents the center of a class of operating states. This weight vector is interpreted as a typical operating state which in this application is given by the line powers. The size of each class depends on the density of probability distribution of the training vectors. The unsupervised training process constructs intermediate classes which do not represent any training vector but may classify unknown system states, thus generalizing information on known states. In addition to the claw information, the 2-dimensional self-organizing map gives a 2-dimensional representation of the n-dimensional operating space. The operating space is presented on the map by secure and insecure regions. A more detailed example is discussed in section 5.

2. .3.2. Choice of Input Data

A power system state can be characterized either by the bus injections or the bus voltages and the topology, or by the line power flows. For training, a set of operating points is obtained either try file.asurcfllcflts or by off-line load flow simulations. The advantage of using bus injections and *line powers.* is that they are available as measurements while bus voltages must be estimated. Line powers contain implicit information on the topology of the network and increase the redundancy. On the other hand, the dimension of the injection vector is smaller than that of the line power vector. This is an advantage when dealing with real-wc~llci power systems.

in addition to unsupervised techniques theft, arc a number of techniques in the literature to reduce the input data, e.g., clustering about typical operating points. A good approach is to use a bounding technique to identify the critical areas of the power system and use that information to reduce the input data input. Another method for selecting inputs is to use the presently calculated security indicators by the EMS system as inputs to the ANN. This will make the ANN act like an alarm processor for the EMS system and thus perform on-line masking in order to reduce the number of false alarms and misses.

2.3. . . . Training

In addition to coil\'er)li(lrli\lly trained neural networks the following improvements have been proposed.

For MLPs partially trained with standard BP methods, reference [Oh *et al.*, 1991] proposes to use query based learning, where new training points are generated with an interval halving method in order to get more accurate performance on a subset of data where the MLP performance is still insufficient. This method works well on noisy input data.

in the 1 lopfield approach proposed in [Kam *et al.*, 1990] the weights are determined with a linear programming approach instead of the sum of outer products of training, vectors, in order to assure a larger stability margin for the convergence of the processing algorithm.

2..3.4. *Performance*

With the exception of [Oh, 1986], where an 196 hrrs system is studied, all reviewed papers work with simulated data usually from small standardized power systems like the IEEE or CIGRE test systems. However *when* working with simulated data ANN can only provide an approximation of the supposedly exact noll-linear power system model and for one specific operating point the prediction of abnormal conditions is as most as good as the ones done hy complete contingency analysis. Presented classification errors rank iu the order of S to 20%.

However more work needs to be done in order to produce better performance. criteria A major step in this direction is proposed in [Yan *et* al., 1994] and discussed iu section 3.4.

Let us now study two examples of a supervised and an unsupervised neural net for static security assessment in more detail

3. A SUPERVISED ANN FOR POWER SYSTEM SECURITY PREDICTION

In order 10 quantify the concept of secure and insecure operating states let us introduce 4 severity levels, Normal, Alert, Emergency I and Emergency 2, as shown in Table 2.

Table 2: Severity Levels

Severity Level	Voltage Drop (%)	Line Flow (in % of emg. rating)	Output Pattern
H_0 : Normal (N)	<4	<80%	d_0 : (0,0)
H_1 : Alert (A)	4.0-4.9	80%-99%	d_1 : (0,1)
H_2 : Emergency 1 (E1)	5.0-5.9	100%-109%	d_2 : (1,0)
H_3 : Emergency 2(E2)	> 6.0	> 110%	d_3 : (1,1)

In the following sections wc will present the design of an ANN-based SA predictor which predicts if the power system is in one of the these 4 severity levels. A 17 bus power system model shown in Figure 1 is used fur illustration of the design and evaluation of the ANN.

3 1. ANN A rchitecture

For the ANN architecture we selected a multi-layered perceptron shown in Fig 2. The main reasons for choosing this ANN architecture over the other ANN architectures is that it is suitable for dealing with nonlinear problems, that effective training algorithm are available, rrnd that outputs of the network can be quantified. The 3-lay ered percepti on consists of the input layer, a middle (hidden) layer, and an output layer discussed in the next sections:

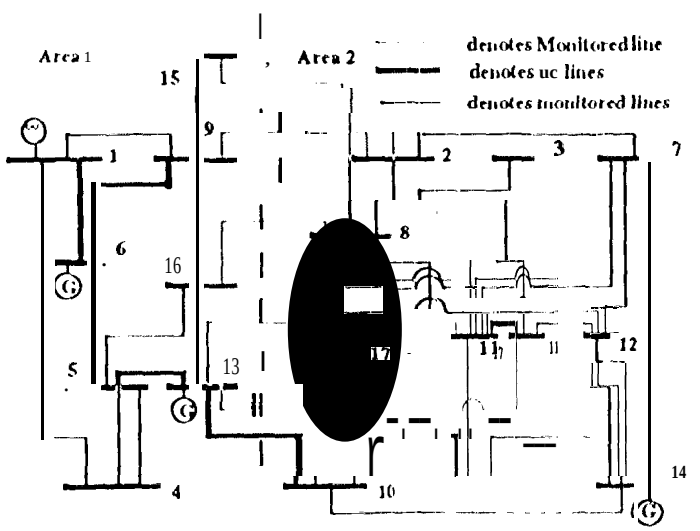


Figure 1: The 17 bus system one-line diagram

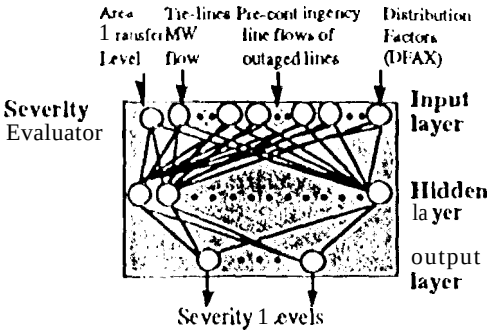


Figure 2: The structure of the Neural Network

3.1.1. *Input Layer*

A general guide for the input layer is that it should include as many neurons as needed for the desired input information. However, as indicated in [Fischl and Chow, 1993], the system data selected for this layer should show close correlation with the output data, Since our objective is to study the thermal overload and voltage drop problems, which arc usually caused hy heavy power transfers, we use the area transfer level (M W), the tic line flows (MW), the pre-contingency line flows (MW) of the critical line outages, and a set of line outage distribution factors (DFAX) as data for the input layer. Based on the above, the input neurons of our NN arc ordered as follows: the pre-contingency area transfer (M W), individual tie line flows (MW), pre-contingency line flow (MW) of the. outage line, and the IWAX of the critical contingencies (p. u.). Thus, for our 17-bus system example with 1 area transfer (between 2 areas), 6 tic. lines, 1 contingency outage (one contingency at a time), and 6 monitored lines, 14 neurons are used in the input layer.

3. 1. 2 Hidden Layer

To date, there is no exact guide. shout the choice of the number of hidden layers and the number of neurons in each layer, although some work has been done in Selecting the number of neurons in the hidden layer [No vosel and King, 1991]. Too many neurons can lead to nlcmoriz.alien of the training sets with the danger of losing the ANN's ability to generalize. On the other hand, a lack of neurons can inhibit appropriate pattern classification To obtain an "optimum" number for the number of neurons in the hidden layer, We varied the number from 20 to 60 and compared the average total errors. For each change in the number of hidden units, the NN was trained one hundred times and the average error for each case was note.d. The results indicate that the optimum number of hidden neurons is somewhere around 40, as improvements in the average errors tend to saturate above this level, We chose 36 neurons in our final design for the hidden layer.

3.1..3, *Output Layer*

ANNs are trained with hinary outputs of 1 and 0. However, in reality, the outputs are closer to analog values in a range [0,1]. Acceptable classifier results can be reset to 1 and O if the output values are >.8 and <.2, respectively. The output layer provides the information on the severity level of the limit violation. For our 17 htrs system, we used 2 neurons to represent the 4 levels of severity.

3.2. *Training Set Selection*

Since training sets are the information required hy the. ANN to develop its expertise, they need to be representative of the different states. We use {Iff-line. load flow results to form our training sets. Considering that in the real world, the exact load-generation profile will differ because of uncontrolled load, changing weather conditions, and other uncertainties, we can assume that the real load-generation profiles to be stochastic and the deterministic off-tine load flow results to represent the expected values of the profiles. As wc only use these expected values for our training data, the need arises for an approach to evaluate the effectiveness of the NN as a means for classification.

For our 17-bus system, the training set consists of off-line load flow results from 9 cases representing area transfers from S22.$ MW to 6337

MW and the corresponding contingency cases. Five single line outages are considered in the study. As noted earlier, the back propagation algorithm is used for the training.

3.3. *A New Prediction Performance Measure*

Recall that for the binary type of security assessment (SA) of Eq.(4), the effectiveness of the SA predictor can be evaluated in terms of P_{fa} and P_m of Eq.(8). This also holds tnrc for ANN-based SA predictor. For the severity evaluator which uses the many levels like those shown in Eq(5), the evaluation process is more complicated because wc must perform multi-hypotheses testing. To do this wc need to quantify the errors made by the ANN if a classification d_s is predicted by the ANN while the severity level is I_k is true. The probability of such an occurrence is the conditional probability that classification d_s is made when the severity level is H_k, i. e. $Pr\{d_s|H_k\}$. Likewise, the probability of a correct classification is $Pr\{d_s|H_k\}$ and the probability of severity level k is $Pr(H_k)$. If there are Ns severity levels in the classification, wc can form a square matrix of size Ns with the diagonal terms representing the correct classification and off-diagonal terms representing the misclassification. Furthermore, if I_s is define.d in order of increasing severity, the $Pr\{d_s|I_k\}$ terms are associated with missed detection and false alarm, when s < k and s > k, respectively.

Ideally, a perfect ANN predictor is rrnc whose $Pr\{d_s|I_k\} = O$ when $s \neq k$. Clearly this is highly unlikely. We therefore suggest the following performance indices and criteria for the evaluation of the performance of ANN-based SA evaluator for security assessment [Yan *et al.*, 1994]:

(i) Local performance indices related to the accuracy of the severity level "k" predictor, PI_k,

$$PI_k = \max\left\{ \frac{Pr\{d_s|H_k\}}{Pr\{d_k|H_k\}}, s \neq k \right\}, k = 0, \ldots . Ns-1 \qquad (9a)$$

PI_k is related to the maximum error of the predictor in correctly classifying the system severity at level "k." For Urc ANN 10 be acceptable for the severity level "k," this PI_k must be less than some threshold val La.', &l, as determined by the designer. We chose $\varepsilon_1 = 0.3$.

$$PI_{km} = \max\left(\frac{Pr\{d_s|H_k\}}{Pr\{d_k|H_k\}}, s<k \right), k = O, \ldots . Ns-1 \qquad (9b)$$

PI_{km} is relatedto the maximum error of missed detection al level "k." For the ANN to be acceptable for the severity level "k," this PI_k must be less than some threshold value, ε_2, as determined by the designer. Wc Chose $\varepsilon_2 = 0.1$.

(ii) Global performance indices related to missed detection, PI_m, rrnd false alarm, PI_{fa},

$$PI_m = \sum_{s=0}^{Ns-1} \sum_{k=s+1}^{Ns-1} Pr\{d_s|H_k\}Pr\{H_k\} \qquad (10a)$$

$$PI_{fa} = \sum_{k=0}^{Ns-1} \sum_{s=k+1}^{Ns-1} Pr\{d_s|H_k\}Pr\{H_k\} \qquad (10b)$$

PI_m and PI_{fa} arc related to the overall performance of the ANN in missed detection and false alarm, respectively. In power system security assessment, an acceptable "predictor" is therefore one that has the least amount of false alarms and nearly no missed detections (i.e., $PI_m = O$) .

If two ANN designs are to be compared, the more desirable one is the ouc with most of the PI_k and PI_{km} terms below the threshold and With smaller PI_m and PI_{fa}. Wc emphasize the word "most" here because certain severity levels arc obviously of more concern than the others to the system operators.

3,4, *ANN Performance Evaluation*

The ANN is evaluate using the following uncertainties in power system operation: The generation uncertainty at hus 1 1has a normal distribution with some mean and a variance of 1.0 p.u., and that the 5 single line outages are equally likely with a 0.2 probability of occurrence. The generation at bus 11was varied to create 3 levels of area transfers, namely high, medium and low transfers.

Based on the method described in [Fischl and Chow, 1993], the Monte-Carlo simulation was used to obtain the conditional probability $Pr\{d_s|H_k\}$ and the probability $Pr\{H_k\}$. The results for the medium transfer level are summarized by the conditional probabilities and the PI_k terms is shown in Table 3.

l'able 3: Summary of the conditional probabilities $Pr\{d_s|H_k\}$ and the probability of hypod

$Pr\{d_s\|H_k\}$	H_0	H_1	H_2	H_3
d_0	0.999	0.000	0.047	0.000
d_1	0.001	0.780	0.007	0.000
d_2	0.000	0.220	0.783	0.000
d_3	0.000	0.000	0.163	1.000

	H_0	H_1	H_2	H_3
$Pr\{H_k\}$	0.204	0,249	0124	0.423

Ideally the matrix shown in Table 3 should only have a diagonal of value onc. This is the case for the prediction of violations of severit y level } I3 where no false alarms and (naturally) no more severe, missed violations arc predicted by the ANN. Values below the diagonal of the matrix shown in Table 3 indicate the probability of false alarms issued by the ANN. Values above the diagonal indicate misses. For example the ANN predicts nonnal operation, i. e. do, instead of emergency 1, i. e. H_2, with a probability of 0.047.

in general an ANN with higher values for the $Pr\{d_s|H_k\}$ terms near the diagonal is better than the. one with lower values. This is because the value of the diagonal terms can be increased, if the "bandwidth" of the severity level can be expanded to include that near diagonal term as part of the "'expanded" diagonal term.

For the classification of 4 severity levels, the ideal case should be that $Pr\{H_k\} = 1/4$. This is approximately the case, as shown in Table 4.

From the values in 'l'able 3 and Eqs. (9) and (10) wc can now calculate the local and global performance indices $PI_k, PI_k^m, PI_m, PI_{fa}$, shown in Table 4 Note that these values are smaller than the constraints ε_1 and ε_2 respectively and the prediction of the ANN is therefore sufficiently accurate

Table 4 Summary of the local and global performance indices for the Severity Predictor /

Local Performance Index	H_0	H_1	H_2	H_3
PI_k	0.001	0.282	0.208	0
PI_k^m	-	0	0.060	0

Global Performance Index	
PI_m	0,007
PI_{fa}	0.075

.$.S *Summary*

The approach presented above uses a probabilistic test methodbased on the classical decision theory. The performance indices can be used to compare the effectiveness of variations of ANN designs in minimizing the probability of misclassification in the security assessment. The individual conditional probability terms from the approach can also be used to uncover arms where design or training improvements can be made.

Based on the proposed method, a good ANN design should have the following characteristics:

1) On the overall performance, the global indices PI_{fa} is below a pre-determined threshold, $PI_m = > O$ and

2) For each level, the local indices PI_k and $PI_k{}^m$ are less than ε_1 and ε_2 respectively.

4. AN UNSUPERVISED ANN FOR STATIC SECURITY CLASSIFICATION

10 illustrate the application of the Kohonen classifier for static security assessment, we briefly present the application of the method for a simple power system as discussed in [Niebur and Germond, 1991; 1992; El-Sharkawi and Atteri, 1993]. The trained neural net provides a two-dimensional representation of the high-dimensional operating space. The evaluation of this map reveals the significant power system features. The terms Kohonen network and self-organi?.ing feature map are used as synonyms throughout this section.

4.1. *Study of a 5 Bus -7 Line Power System*

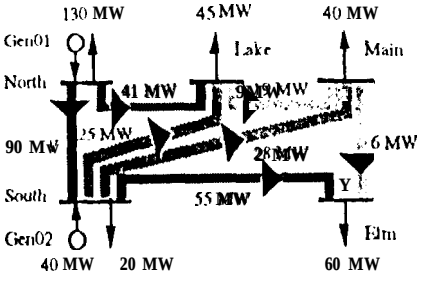
The Kohonen network is used 10 classify line loading patterns resulting from single and double contingencies for a 5 bus -7 line power system represented in Figure 3. The input vector representing the operating state is defined by 7 complex components or, alternately, 14 real components, the 7 active and reactive line power flows. For brevity, the lines in Figure 3 will be designated by the first letter of the busses connected by this line, *e. g.* Line North-Lake is called N-1,:

One load and generation scenario was defined as the base case. The 46 training vectors were obtained by of(-line load-flow simulations of all n-1 and n-2 contingencies using the non-linear power system model. These 46 vectors can also be viewed as 46 different line loading patterns corresponding 1046 different power system topologies.

The information on the bus power injections is implicitly present in the input vector since the power on the lines connecting to the same bus will add up to the bus power. 'Ibis means that the input vectors lie on a manifold of the vector space. Therefore the actual dimension rrf the operating space is smaller than twice the number of lines.

The information 00 the bus voltage is implicitly present in the input vectors as a rmn-linear dependence (the load flow equation). The.sc can he looked up in the data base for the trained cases.

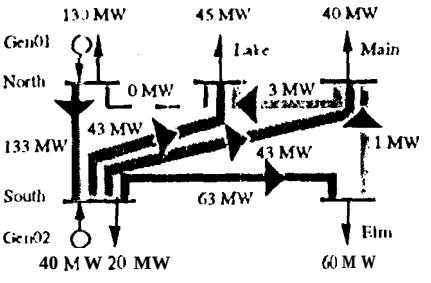
Figs. 3, 4 and 5 show the base case, N-1. contingency and N-S contingency for the 5-bus system respectively. Only the active power flow has been reported in the network presentation. The operating vectors include active and reactive powers.



Operating vector	
1 N-L	41 MW
2	-2 MVAr
3 N-S	90 MW
4	.30 MVAr
5 s-E	55 Mw
6	9 MVAr
7 S-M	2s MW
8	s MVAr
9 S-L	25 MW
to	6 MVAr
11 L-M	19 MW
12	-7 MVAr
13 M-B	6 MW
14 -3	MVAr

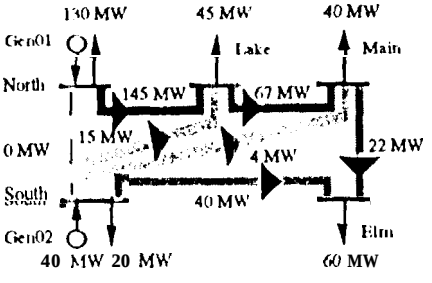
Figure 3: The power flow of the base case. The darkness of a line's shading increases with its load.

Bus North serves as the slack bus. Bus South is a voltage regulated bus of type PV and all other bosses arc load busses of type PQ.



Operating vector	
1 N-L	0 MW
2	0 MVAr
3 N-S	133 MW
4	-40 MVAr
5 S-E	63 MW
6	to MVAr
7 S-M	43 MW
8	7 MVAr
9 s.1.	43 MW
o	8 MVAr
1 L-M	-3 Mw
2	-7 MVAr
3 M-B	-t MW
4	-3 MVAr

Figure 4: The power flow for the contingency of line North-Lake. A line outage is represented by a dotted line, an overloaded line by a black line.



Operating vector	
1 N-L	145 MW
2	-4 MVAr
3 N-S	0 MW
4	0 MVAr
5 S-B	40 Mw
6	18 MVAr
7 S-M	-4 MW
8	22 MVAr
9 S-L	-15 MW
10	30 MVAr
11 L-M	67 MW
12	-33 MVAr
13 M-B	22 MW
14	-11 MVAr

Figure 5: The power flow for the contingency of line North-South.

The base case and contingencies lie in different manifolds of the. operating spare, Assuming a maximal tolerated active power of 100 MW for each line, N-S contingencies result in N-1. overloads and vice versa.

4.2. *Training of the Feature Map*

A 7x7 self-organi?.ing map has been trained with 46 single, double and mixed contingency operating states which were presented several times in random order. After about 4000 steps of learning, the network is already organized, i. e. the weight vectors have converged to an equilibrium point of the neural system.

4.3. *Evaluation of the Cluster Map for Training and* lest *Data*

In order to evaluate the classification results, a set of test vectors has been generated at a' "reasonable" distance from the 46 trained vectors through uniform variation of load and generation at 90%, 95%, 105%, and 11 O% of the total load of the base case. The claim of a reasonable distance is justified hy the practical consideration that load and generation for a network usually vary around a scheduled case. 184 untrained single and double contingencies were presented to the Kohonen classifier. Figure 6 shows the. cluster map for the classification of the 184 untrained vectors.

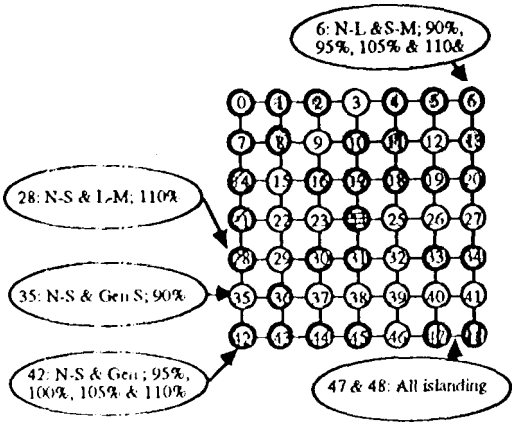


Figure 6: Cluster map of the classification of 180 test vectors for the 5-bus 7-line system indicating contingencies classified by selected neurons

Neurons shaded with the same pattern classify at least one test case. They belong to the same cluster and classify the same type of security violation, for example neuron 42 and neighbors classify N-S contingencies resulting in N-1. overloads. **Neurons marked by hold circles classify at least one training** case. Neurons with empty cases do not classify neither training nor the test vectors. That means their weight vector has never hccn chosen as the closest vector to any of the training or test vectors.

Several different clusters can be distinguished. Normally loaded situations arc classified by neuron 33 and its neighbors. Neurons in the upper right corner, i.e. neuron 6 and its neighbors classify N-I. contingencies resulting in N-S overloads. Neurons in the lower left **corner, i. e.** neuron 42 and its neighbors classify N-S contingencies resulting in N-I. overloads. Islanding is classified by neuron 46 and 47. The set of neurons classifying test cases includes the set of those classifying training alone. Note that operating in different subspaces, i. e. N-1. and N-S contingencies arc classified by neurons situated far away from each ofher on the map.

4.4. *Classification Error for the Test Set*

For the 184 untrained cases the total error rate, including fake alarms and misclassifications, is about 8.4% whereas the misclassification rate alone is only 4.4%. All neurons involved in misclassification indicate a security violation for at least ouc component and therefore already present unsafe operating points. If we are only interested in unsafe versus safe cases, **there would not be a single misclassification** in this test set, because the most significant overload situation is always detected correctly. The wrong classification may however occur for a less significant overload of another line. The misclassifications never declare an unsafe state to be safe, hut the magnitude of the apparent power of one line would be wrongly predicted as not overloaded in 4.4% of the test cases.

A second test set was generated, taking 20 base cases with loads varying individually in the range from 75% to 125% of the trained base case. Simulation of all single and double contingencies thus yields shout 900 test vectors. The classification error for false alarms is in the order of 7.43%, the misclassification error is 3.35%. Once again in 2.4 % of the misses occur for operating states involving two or more overloads where the severe overload of a line is correctly predicted and the second less severe overload is missed. Only in 0.7% of all cases the ANN **predicts normal operating** for all lines thus missing a present overload. The significant percentage of the false alarms occurs at border neurons of unsafe clusters.

4.5. *Interpretation of the Weights*

Each neuron of the Kohonen map can he associated with its weight vector which represents a prototype of a class of input vectors. However, some neurons never classify any training vector. We therefore need a procedure to establish the security class represented by these weight vectors withoot any a-priori information on the test vectors which might be classified by these neurons.

The weight vectors themselves are calculated as a weighted sum of a certain number of input vectors which form a class. Therefore, with our choice of variables for the components of the input vectors, each compo nent of a weight vector represents either an active or a reactive line power flow. For example, the first component of every weight vector corresponds 10 the active power in the branch North-1 ake.

In order to analyze the weight vectors we do *not* need any information on the class of input vectors. The features of these classes are directly represented by the **values of the weight vectors.**

In Table 5, three out of the 49 weight vectors are represented. Neurons 5 and 6 arc neighbors in the feature map (see Figure 6) and the weight vectors arc close to each other with respect to the Euclidean distance. Note that weight vector S represents the single outage of N-1., whereas vector 6 represents the double outage of N-I. and S-M. Neuron 45 is situated relatively far away from neurons S and 6 and represents a contingency of line N-S resulting irr an overload of N-1..

Table 5: Weight vectors of neuron S, 6 aad 45.

Line	Weight vector of neuron 5 (MVA)	Weight vector of neuron 6 (MVA)	Weight vector of neuron 45 (MVA)
N-L:	0.0 + j 0.0	0.04 j 0.0	118.9 . j 4.5
N-S:	138.4 - j42.1	135.3 - j41.5	0.0 + j 0.0
S-E:	62.2 + j10.1	79.6 - j17.4	40.0 + 516.8
S-M:	42.7 + j 6.2	0.0 + j 0.0	-2.4 + 522. s
S-L:	44.2 + j 9.7	71.8 + j18.9	-13.4 + j28.2
L-M:	-2.1 - j5 .2	23.5 - j 2.4	64.4 - j31.0
M-E:	-0.6 - j 2.1	-16.6 - j5.8	21.1 - j10.7

Let us now consider the third component of all weight vectors, corresponding to the active power of line N-S, *i.* c. the rest part of the complex number in the highlighted line in Table 5. This component is represented for all 49 neurons in a three-dimensional representation *on* the left hand side of Figure 7. The 49 neurons are distributed equidistantly on the vertices of the square-lattice in the *xy* plane (some of the border neurons have been labeled with their number), and the "z"-dimension represents the third component of the weight vectors. Those neurons in which this value (i. *e.* the active ***power on line N-S)*** exceeds the maximally allowed value are marked hy dark circles, and neurons with very weak loads (usually corresponding to outages) are marked by white **circles.**

It is seen in this representation that the N-S component of neurons 28, 35, 42 to 45 and 48 is extremely small, Since input vectors corresponding to N-S outages will have the corresponding vector component equal to zero, the neurons mentioned above will likely be close to these cases and therefore classify N-S contingencies. We have already seen the case of neuron 4S which indeed classifies the single outage N-S.

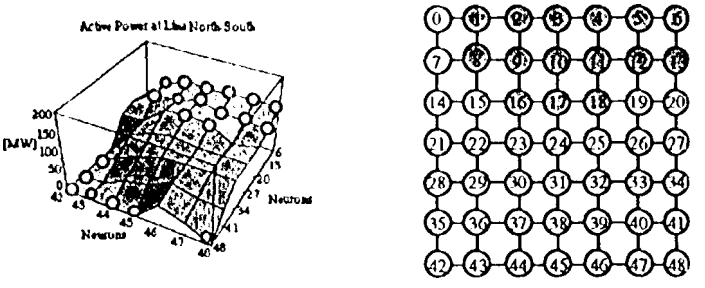


Figure 7: Three-dimensional view' of the 49 weight vector components corresponding to the a live power flow of 1 me North-South and corresponding flat component map.

If we assume again an active power limit of 100 MW for line N-S, the **compar ison of this limit to the corresponding weight vector component** of neuron i indicates whether neuron i classifies system states that arc likely to violate this limit. In the discussed example, **neurons** 1-6,8-13 and 16-18 have N-S components exceeding the given limit and will most likely classify cases tori esponding to N-S overloads. We report the components indicating overloads on the two-dimensional grid of our 7x7 feature map to the rig.ht-hand-side of Figure 5, thus establishing a *component map* for line N-S. Also in this representation, overloads are marked by dark shading of the corresponding neurons (we do not mark outages explicitly).

We proceed in the same manner with the other 13 components of the weight vectors. By analyzing these component maps, the properties of neurons not classifying any of the training vectors can he determined. For example neurons 3, 11, 12 and 13 will also classify overloads of North-South, they need not classify any of the training vectors. We will call this the generalization capability of the feature map.

4.6. The *Cluster Map* - An *Assembly of the Component Maps*

This synthetic representation of the properties of the weight vectors is usually called cluster map. It corresponds to the top layer in Figure 8 which illustrates schematically how the cluster map is assembled.

The top map is the combination of all lower (component) maps. For each weight vector component there is one component map, only four of t h e m being shown.

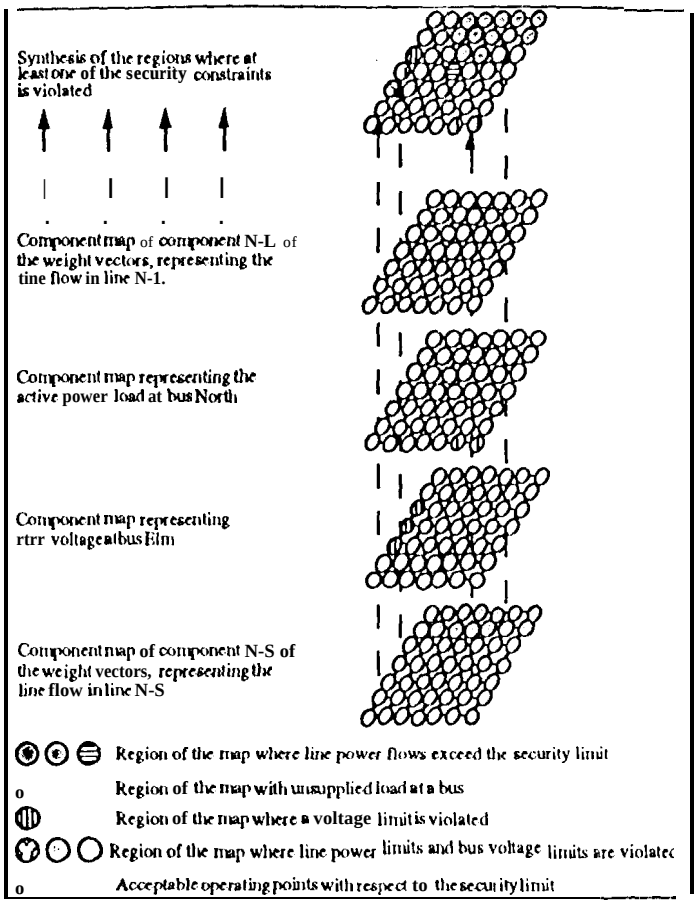


Figure 6: Generation of the cluster map.

The cluster map is generated as a superposition of the component maps established from the analysis of the weight vectors *(only* four of the components maps are shown schematically). The 7x7 neurons on the component maps are situated as usual on the crossings of the horizontal and vertical lines. The qualitative information of secure and insecure neurons can be coded as patterns or *colors.*

For the cluster map, wc have used exclusively information from the weight vectors. We would like to emphasize, that it is one of the. crucial advantages of the self-organizing feature map technique that a-priori information on the test vectors is 001 necessary to classify the system states. The unsupervised learning algorithm reveals the underlying structure of the input data without requiring any explicit knowledge about the system.

4.7. *Summary*

The classification of power system slates with the self-organizing feature map can be summarized as follows:

1) The neural net is trained off-line with one or several base cases and the related *n-1* or *n-2* contingencies. These contingencies can equally be regarded as different topologies of the power system.
2) An unknown operating state is presented in real time to the neural net. The neural net considers this state as a base case and will classify this case by a prototype state, e. *g.* weight vector 33.
3) Knowing that e. *g.* all contingency of line N-S of the vectors of class 33 will lead to an overload in line N-I. the neural net draws similar conclusions for all *n-1* or n-2 contingencies of the unknown operating state. If the. unknown operating state corresponds already to a different topology obtained from the base case hy taking onc line out, then conclusions can be drawn for all single contingencies of the case provided all *n-2* contingencies have been trained.
4) If during power system operation the classification of the operating state moves from neuron 33 over to neuron 25, the neural net further indicates that the trajectory of the operating point moves towards an overload situation concerning line N-S or line S-E.

There are several advantages to this approach:

a) There is no need to run a contingency analysis in real time and therefore the problem of combinatorial explosion can be avoided during operation.
h) The classification of a case is extremely fast, since it only requires the evaluation of a limited number of distances.
c) In addition to the classification of the present state, the trajectory of the operating states predicts the overall tendency for future operating states allowing early preventive action to be taken.
d) In traditional control centers, the operating situation is presented either alphanumerically or by colored graphs of the power system, often containing hundreds of distinct, differently colored lines. The relation between a contingency in line *a* and an overload in Line *b* can neither be directly concluded from the graph nor from the numbers although experienced operators would know them for the most common operating situations. The two-dimensional map regroups these relations into distinct security areas thus exhibiting the qualitative behavior of the power system even for unusual operating situations. These maps can be ideally displayed on a color terminal.

5. ARTIFICIAL NEURAL NETWORKS IN DSA

5.1. *Overview of ANN for Dynamic Security Assessment*

Although dynamic security is defined as security with respect to transient stability, there are many instances where it has been used with dynamic stability connotations. Dynamic stability of a power system is determined by the eigenvalues of the linearized state space model of the system generators. *Presence* of eigenvalues with positive real components indicate dynamic instability. However, eigenvalues are susceptible to changes in operating point and topology of the power system and have to be frequently re-evaluated at significant computational cost. in [111 -Sharkawi *et al.*, 1989], a neural network approach to predict the dynamic stability status of a power system was proposed. A layered perceptron was trained to *learn the* implicit mapping between varying system operating states such as real and reactive injections at selected buses and the corresponding dynamic security status. The trained neural network was used to create 2-dimensional security contours with respect to the selected system attributes.

A similar concept but for a Kohonen net is proposed in [Mori *et al.*, 199 1]. The inputs to the neural network were the d-q axis voltages, rotor angles and speeds of the individual generators. The output was a 900 neuron (30x30) 2-dimensional grid. This grid was divided into 10 different areas based on *the* magnitude of the largest eigenvalue within the unit circle. Hence the output was indicative of the degree of security rather than a binary security index as with [Fischl *et al.*, 1989].

The concept of *critical clearing time* (CCT) is also a measure of dynamic security of a power system. However, it is a complex function of the power system topology, load level, and fault characteristic. The calculation of CCT involves considerable computational cost. In [Sobajic and Pao, 1989], a technique was proposed where a layered perceptron was trained to predict the CCT for a fault based on the pre-fault system attributes, such as the acceleration powers and the relative load angles of individual generators, The training patterns were generated for different load levels and base topologies. The corresponding CCTs were derived by numerical integration of the system state equations. It was proved that the neural network can generalize its knowledge to previously unencountered system topologies and load levels and predict the CCT with reasonable accuracy. In a follow up [Pan and Sobajic, 1991], a combined unsupervised/supervised learning algorithm was proposed to solve the same problem. The input data was pre-processed using an unsupervised clustering algorithm in order to enhance the accuracy of the supervised learning algorithm. A separate set of features were selected for each cluster based on the covariance matrix.

It was pointed out in [Kumar *et al.*, 1991; CEI, 1994] that most of the research done up to date *in the* area of dynamic security were conceptual investigations and as such, they had impressive results. It was noted however, that considerable progress has to be made before these techniques are applicable in a realistic on-line security assessment

package. The major obstacles arc the dimensionality and the combinatorial complexity of a real power system. Kumar, *et al., [* 1991] proposed a hybrid expert system/neural network approach which can effectively utilize the existing high level knowledge of the system operators while training neural networks to execute the more uncertain lower level tasks.

5,2. Promising are as

The prime candidates for application of neural networks are in the subproblems of DSA which require generalization of the results of cases studied by engineers, to the many potential situations that cannot be studied. Some of the obvious candidate subproblems arc in [Kumar *et al.*, 1991; CEI 1994]:

in *contingency selection, to* identify potentially severe outages based on the current operating state.
in *contingency screening,* to identify definitely harmless and potentially harmful contingencies.
in determining conditions for termination of time domain simulations.
in determining pre-contingency transfer limits

6. CONTINGENCY *SCREENING* BY LAYERED PERCEPTRONS

Contingency screening is a fast approximate method of determining, whether a contingency has the potential to cause security violations. The proposed mrslti-layered contingency screening approach is given in Figure 9. Screens at each level have significantly different capabilities and accuracy in detecting contingencies with potential violations. Neural networks arc selected for one level of screening. Layered perceptrons are trained to identify dynamic security with respect to a selected set of contingencies based on pre/post contingency system indices. The approach has a striking similarity to that for static security. However some real issues with respect to dimensional and combinatorial complexity need tobe addressed.

Each pre-contingency configuration gives rise to many post-contingency configurations.
Generation schedule of the power system is a function of many factors that may not all be identified.
The number of possible system configurations is large.
The number of available training cases are relatively small.

The first issue is unique to dynamic security. For example, the same pre-contingency power system can be either secure or insecure depending on how soon the fault is cleared. Therefore, security cannot be estimated based solely on pm-fault features. One way to deal with the problem is to derive a set of indices (features) which describe the condition of the power system immediately following fault clearing, in terms of the pre-contingency steady state. The elapsed time prior to fault clearance will he implicitly captured through deviation of the indices. Moreover, the features should not be too sensitive to the system configuration and then have the neural network generalize among the unseen topologies. Following arc some of the suggested guide lines for generating features for security studies [Kumar *et al.*, 1991; CEI1994]:

Calculated for each component of the system.
Raised to a high degree to accentuate the difference between small and large values and thus reduce the effect of masking.
Normalized to make them configuration independent and to avoid numerical overflow problems.
Averaged out over the relevant components.

A set of high level features defined under the above guidelines are described below [Kumar *et al.*, 1991; CEI 1994].

The risk to the system security through increased generation and lower system voltages are captured by,

generator real power output (normalized by inertia)
generator reactive power output (normalized by inertia)
generator apparent power (normalized by inertia)
generator bus voltage
generator rotor angle with respect to center of inertia
generator $(Q - Q_{bias})/P$

The effects of increased line loads. the vulnerability of the "down stream' system scan from the generator are captured by at tributes,

line sending end real power (normalized tsy line reactance)
line sending end reactive power (normalized by line. reactance)
- hoc phase angle
line sending end $(Q - Q_{bias})/P$

The effects of low bus voltages, high bus loads, high power transfer across pre-specified interfaces and overall system loading are captured through attributes,

bus load (normalized by the line admittance)
- bus voltage
real power flow in pre-specified interfaces (normalized by the admittance)
reactive power flow in pre-specified interfaces (normalized by the admittance)
system reactive power generation (normalized by total real power)
- system stress

In addition, the following variables describing the transient conditions immediately following fault clearance may also be needed.

change in speed of generator
change in kinetic energy of generator
acceleration of generator
approximate potential energy of generator
approxlmate enei gy ratio
speed of system center of inertia

Since the indices are averaged over the relevant components, the number of indices are independent of the size of the power system. This is specialty useful in dealing with large scale power systems.

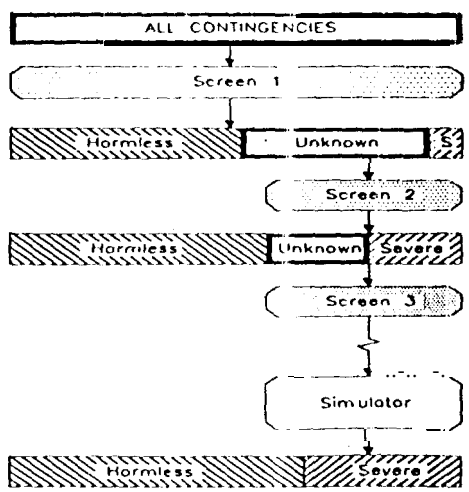


Figure 9. Multi-layered contingency screening

7. CASE STUDY

EPRI, ABB-Systems Control and the University of Washington cooperated in a feasibility study on the applicability of NN to the security assessment [Kumar *et al.*, 1991; CEI 1994]. In this study, the dynamic security of an equivalent test system of Ontario-I Hydro (OH) is investigated under 6 specified faults using layered perceptrons. Training data for combinations of 7 different load levels and 9 different clearing times totaling 63 (9x7) patterns, are given under each fault. The corresponding dynamic security flag (secure=0, insecure=1) is also given. The security contours of each contingency as a function of load level and clearing time arc given in Figure 10. The training data were generated on transient analysis programs of ABB Inc. The preliminary study was for security classification under two conditions: with and witbout the knowledge of Contingency.

7.1. Contingency and Topology Specific Classification Without Feature Extraction

In this study, 6 individual neural networks were trained to assess dynamic security under 6 contingencies. 63 patterns characterizing each contingenc y were derived from the same base topology of the steady state power system. Each pattern contains 28 attributes derived from the previously specified list of features which were measured at the point of fault clearing.

Each data set was normalized between O and 1, and randomly shuffled to remove any bias towards the selection of training and testing data. Table 6 gives the common architecture and learning parameters of the contingency specific neural networks.

Table 6 Neural Network Parameters

Architecture	Learning statistics
input dimension = 28	L-arming step = 0.05
output dimension = 1	momentum = 0.05
hidden layers = 1	training patterns = 50
hidden neurons = 8	testing patterns = 13
	iteration sweeps = 1000

Table 7 gives the classification performance on the training and testing sets under each contingency. For cacb neural network, the actual ratio of secure and insecure patterns for the corresponding training and testing sets are given. The classification accuracy is given by the number of false alarms and misses.

Table 7 Classification Results

	Training Set		Testing Set	
Contingency	secure/insecure	alarms/misses	secure/insecure	alarm.dmiwes
1	33/17	0/0	9/4	0/1
2	24/26	0/0	8/5	0/0
3	12/38	0m	5/8	0/0
4	50/()	0/0	13m	0/0
5	44/6	0/0	12/1	0/0
6	45/5	0/0	11/2	0/0

A graphical interpretation of the neural network output under each contingency is given in Figure 10. Contingency 4 is omitted since it has no insecurities as seen from Table 7. A mesh plot of the neural network output surface for the 63 patterns is given on the left. On the right, the contour of the neural network output threshold (0.5) (—) is superimposed on the actual secure/insecure corridor (-----) of the corresponding contingency over all combinations of load levels and clearing times.

It is interesting to note that *none* of the contingencies had false alarms. 1 lowever, under contingency 1, the neural net threshold intruded into the insecure region as seen in Figure 10 (a) on the next page. This tends to produce false dismissals which was confirmed by the classification performance in Table 7.

7.2 *Topology Specific Classifications with Feature Selection*

Following the success of the previous test, an enhanced set of 52 features were used to describe the same fault phenomena. These new features were introduced to unmask the sign of the previous indices which disappeared when raised to a higher degree as explained earlier. The enhanced features would enable the use of a single neural network to classify security under all contingencies. All other dynamics remained the same.

Two neural networks were trained for security classification: the first used all S2 attributes as inputs. and the second used 24 features selected through the feature extraction algorithm described earlier. The training and testing data sets for both neural networks had the same consistency. They were obtained by randomly shuffling the initial 378 patterns 152S6 times. The first 300 patterns *were* used for training and the remaining 78 patterns for testing. The random shuffling was done to ensure that data corresponding to all contingencies, load levels, and clearing times were randomly allocated to the training and testing sets. Table 8 presents the training and testing statistics for the two neural networks

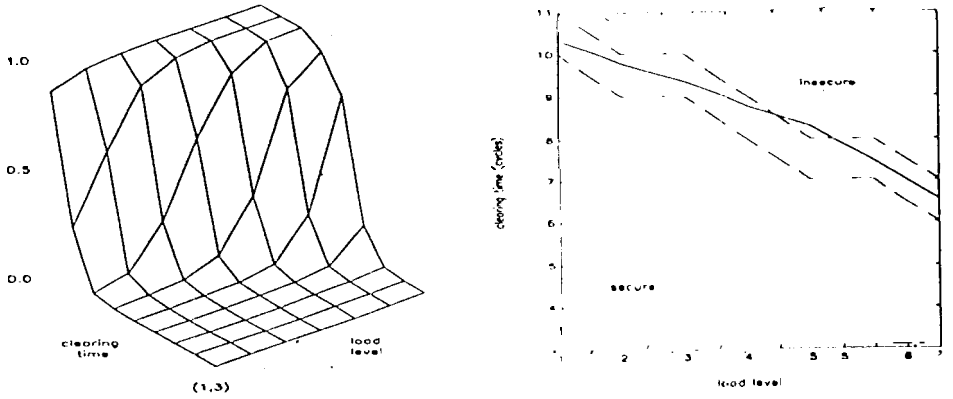
Tabk 8 Neural Network Training and Testing Data

Neural network training and testing	without feature selection	with feature selection
Architecture		
inputs	52	24
outputs	1	1
hidden layers	1	1
hidden neurons	3	3
Learning		
learning step	0.05	,0.05
momentu ni	0.05	0.05
iterations	2700	3600
CPU time (sec)	88.38	42.9
Performance		
training data	300	300
secure data	210	210
insecure data	90	90
false alarms	2	t
false dismissal	2	o
training error	1.754	1.757
testing data	78	78
secure data	56	56
insecure data	22	22
false alarms	1	1
false dismissal	0	0
testing error	0.561	0.557

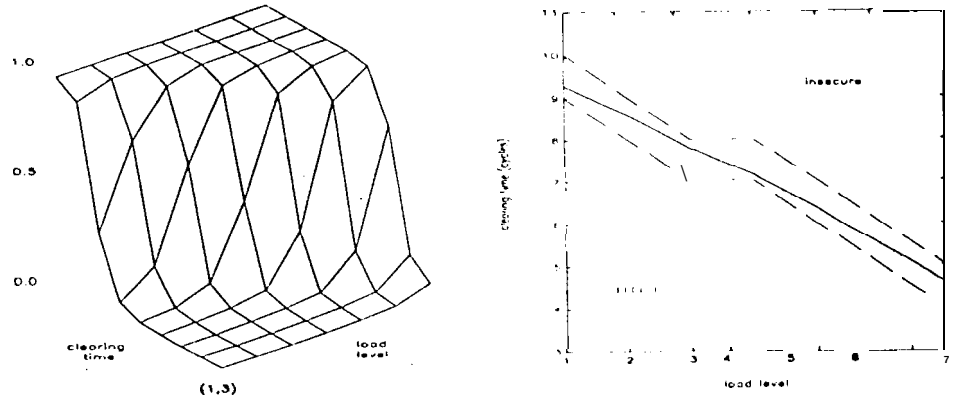
For comparison, the same training parameters were used in both cases. Both neural networks were trained until the same training error (E) was obtained. The variation of training error *E vs. the* number of iterations were plotted in Figure 11. It is interesting to note that the neural network trained with selected features took more iterations to achieve a comparable error. however, due to ifs compact architecture, the CPU time used during training was lower. Moreover, as seen from Table 8, improved overall classification performance on the training and testing sets indicate a superior generalization capability through the use of feature selection.

Figure 12 presents a contour plot of the output surface of the neural network trained with the 24 selected features, with respect to tbc 5 non-trivial contingencies. They were generated as described under Figure 10. Besides the 0.5 threshold contour, those corresponding to 0.4 and 0.6 were also plotted in order to investigate the degree of confidence of the neural network classifications.

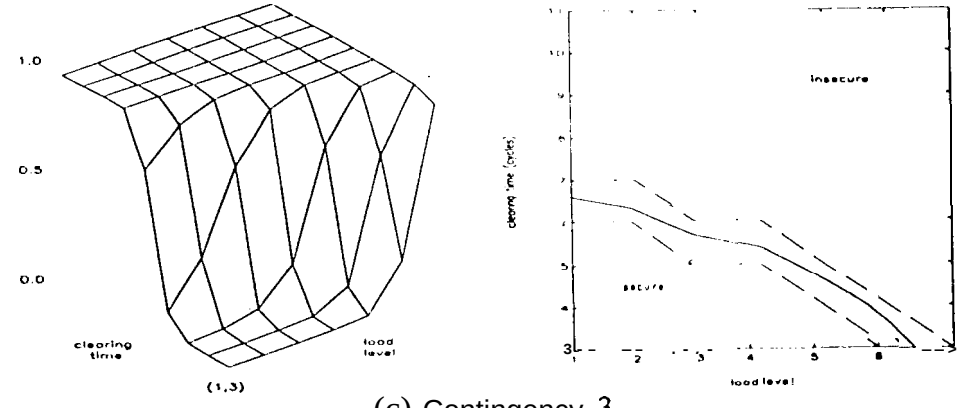
It can be seen from the 5 contour plots that neural network displays the best performance when classifying contingencies 3 and 5. In this case, both 0.4 and 0.6 contours arc witbin the security corridor.



(a) Contingency 1

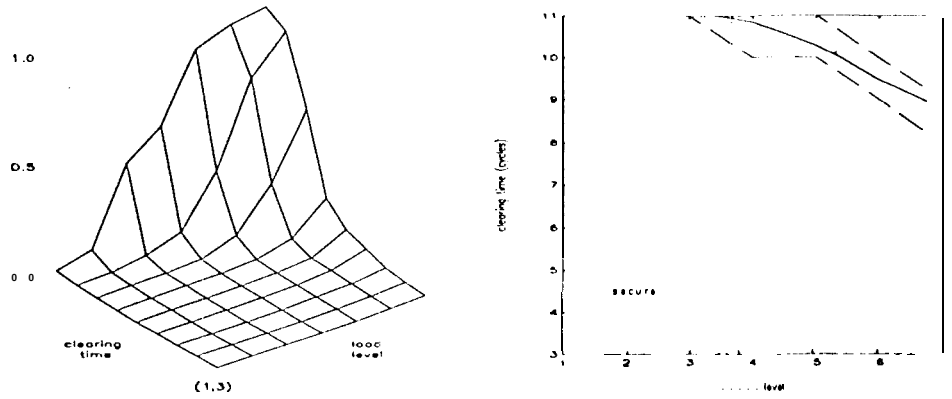


(b) Contingency 2

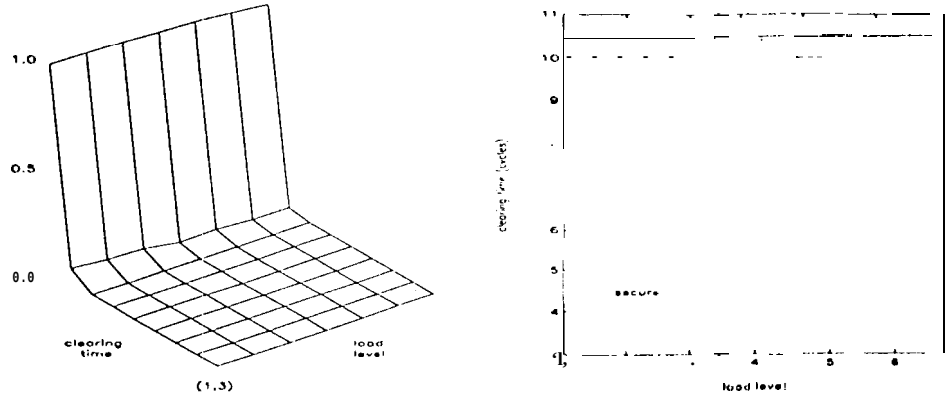


(c) Contingency 3

Figure 10. The neural network output as a function Of load level and clearing time with the corresponding contour plot



(cl) Contingency 5



(e) Contingency 6

Figure 10 (cont): The neural network output as a function of load level and clearing time with the corresponding contour plot

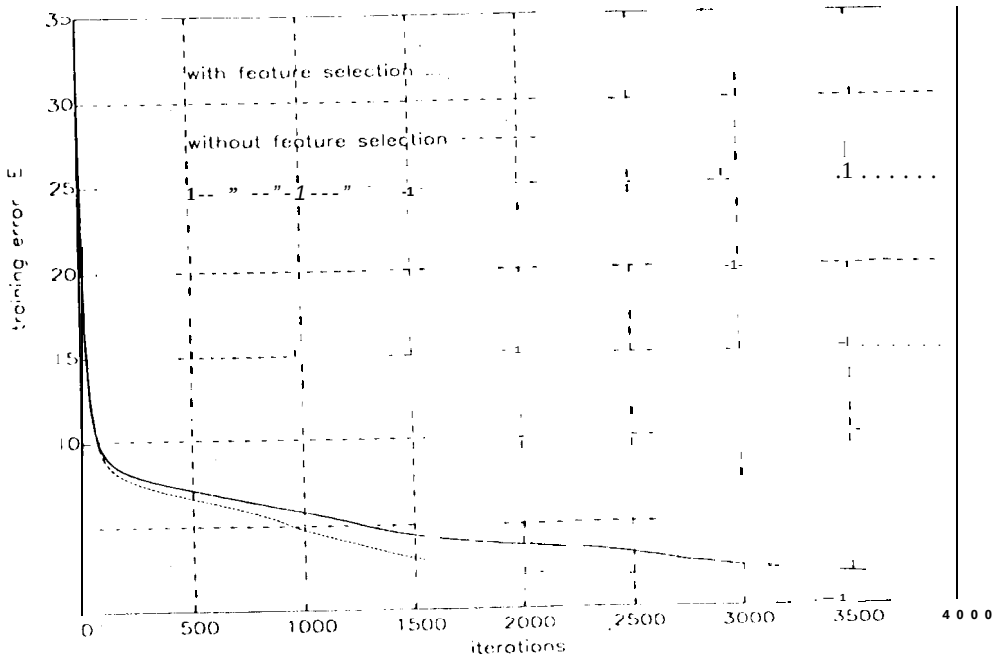
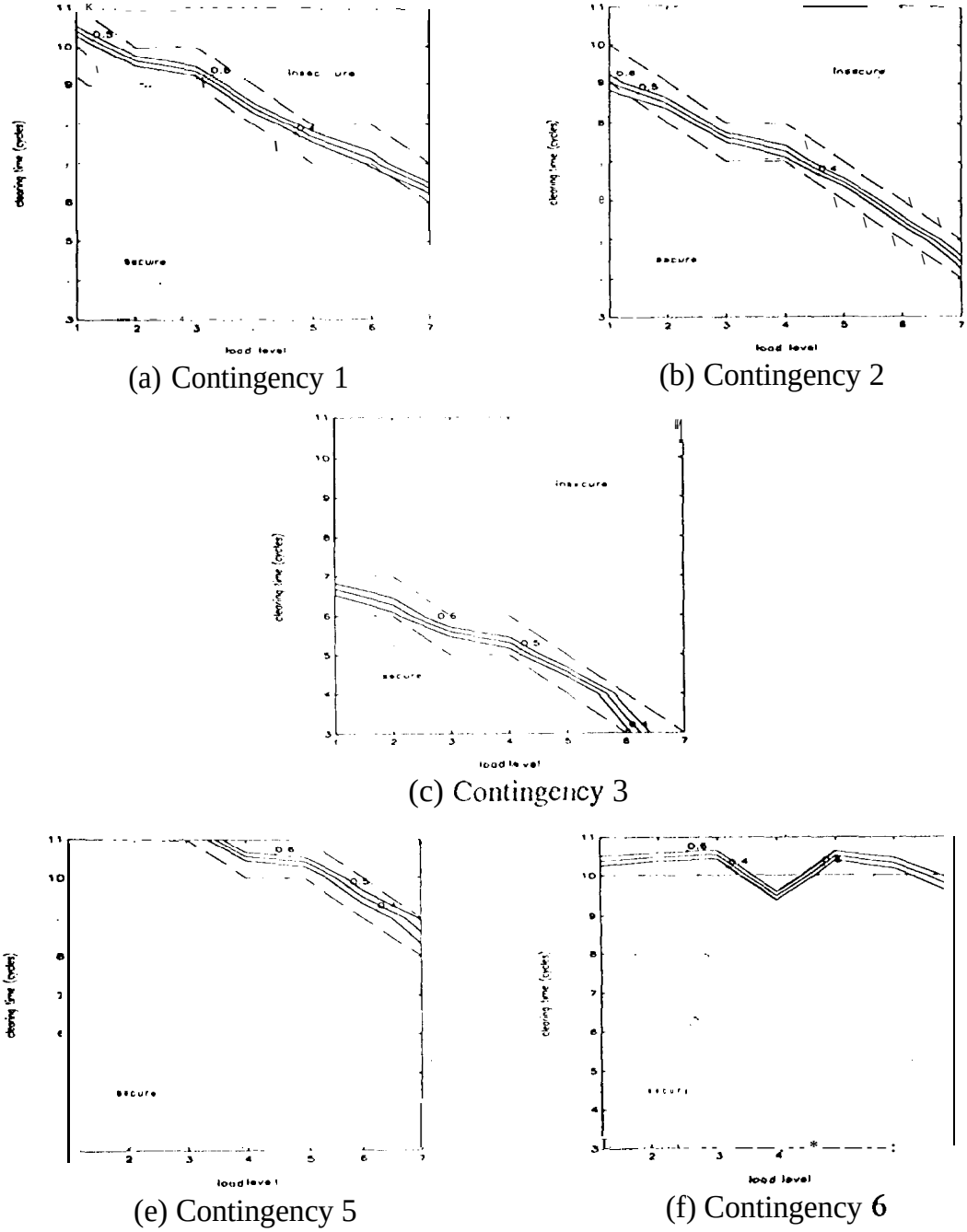


Figure 11: Variation of training error for the two neural networks



(a) Contingency 1 (b) Contingency 2

(c) Contingency 3

(e) Contingency 5 (f) Contingency 6

Figure 12: Neural net work predictions under individual contingencies

Under contingencies 1 and 2, the classifier is biased towards producing false alarms. However, the given data set is classified free of errors. Both false alarms that are encountered in 'l'able 8 seem to occur under contingency 6. however, the fact that there are no false dismissals is an encouraging sign of the neural network's ability to generalize among contingencies.

8. CONCLUSION

8.1 Summary

Security assessment is formulated as a classification problem where trained ANNs arc used as classifiers. The motivation is to usc the concepts of pattern recognition to improve the speed of security assessment computations.

Most artificial neural net approaches solve a more global task then classical security assessment in which the contingency classification, ranking and evacuation are the primary problems. They attempt to find a global description of the operating space (or parts of it) and its security boundaries. As statistical tools they depend heavily on good statistical representation of the operating space.

Since the security analysis problem is of high dimensions, most ANN methods suffer from the combinatorial explosion of the number of contingencies in the same way as classical methods. However, because of their parallel computational approach this problem is more severe, and some type of partitioning and sequencing needs to be made. When comparing supervised and unsupervised ANNs, wc note that they have different objectives. Unsupervised approaches usually divide the operating space into classes of operating points, thus pre-processing the data set by reducing it into a limited number of typical cases. These cases can then hc evaluated either with standard methods or with

supervised learning. Supervised approaches attempt to approximate the security boundaries or the operating space, thus memorizing datapoints of a high-d imensional function and interpolating between them.

For high-dimensional operating spaces, it is not feasible to generate a sufficiently large, statistically significant training set for the complete set of operating points. In daily operation, only a limited number of operating situations are planned. The set of training vectors will be generated by training with input vectors selected randomly from the region of the scheduled operating points. If these operating points change significantly, some types of neural networks have to be trained again, even daily, if necessary. (Of course, the weight vectors of trained networks can be stored off-line and used again for similar operating conditions.) In contrast to many other neural net applications, training time is a crucial issue in power system security assessment. An efficient implementation of Kohonen networks on specialized hardware is discussed in [Cornu et al, 1994].

8.2 *Challenges*

When NN is used, the investigated issues should include:

Problem partitioning that incorporate neural networks to expedite security calculations while preserving the advantages of conventional problem solving paradigms.

Oracle and support software which can extract features from the pre/post-contingency power system information with respect to different systems, topologies, and configurations.

Statistical feature selection techniques to reduce the dimensionality of the input data while preserving classification accuracy. This would complement the higher level feature selection that may have already been performed through expert knowledge.

Capability of neural networks to correctly classify and generalize security among correlated and uncorrelated loading. conditions. This is contrary to a conforming load model that has been used in most literature to date.

Selection of neural network architecture and learning algorithm, such as net size, learning step, number of training patterns, and iterations, based on the distinctive features of the problem such as size of power system, nature of contingency, and number of violations.

Ability of the NN to generalize among different contingencies and operating.

Ability of the NN to recognize the secure region in the operational scram.. In other words, the NN should be able to perform a contour tracking of the secure region.

Future research needs to focus more on adaptive learning techniques and ancillary techniques, as discussed in [El-Sharkawi, 1995], in order to break down the dimensionality of the assessment task.

Finally, one needs to develop ANN design procedures which will optimize the performance of the ANN in terms of the security assessment problem, i.e., minimize the performance indices suggested in Section 3.5.

9. ACKNOWLEDGMENTS

This research reported by the first author (R. P.) was supported in part under NSF Grant, ECS-8922142.

The research reported hy the second author (D. N.) described in this paper was started at the Swiss Federal Institute of Technology, Lausanne (EPFL), sponsored by EPFL, and was completed at the Jet Propulsion laboratory, California Institute of Technology, sponsored by the U.S. Department of Energy through an agreement with the National Aeronautics and Space Administration.

Reference herein to any commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, dots not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

The third author (M. E.) would like to acknowledge the work of his previous graduate students: Dr. Siri Weerasooriya, Dr. S. J. Huang and Dr. D. C. Park.

10. REFERENCES

GENERAL INI'ORMA'I1ON AND OVERVIEWS

N. Balu, *et al.*, "On-line Power System Security Analysis," Proceedings of the IEEE, Vol 80, No. 2, February 1992, pp. 262-280,

CEI Report, "Potential Use of Neural Network Techniques far On-Line Dynamic Security Assessment of Power Stations," Canadian Electric Association report ST-347C-P, 1994

J. C. Chow, Q. Zhu, R. Fischl, and M. Kam, "Design of a Decision Fusion Rule for Power System Security Assessment," *IEEE/PES* 92 SM 600-7PWRS.

CIGRE TF 38-06-06 on Artificial Neural Network Applications for Power Systems, Dagmar Niebur (cm veaer), "Neural Network Applications in Power Systems," Int Journal of Engineering Intelligent Systems, Vol. 1 No. 3, pp 133-158, December 1993.

M. J. Damborg, M. A. El-Sharkawi, M. E. Aggoune arrd R. J. Marks II, "Potential of Artificial Neural Networks in Power System Operation," IEEE Proc. of 1990 ISCAS, pp. ?9332937, New Orleans, Louisiana, U. S. A., May 1990.

M A. I l-Sharkawi, *et* III., "Neural Networks and Their Application to Power Engineering," Control and Dynamic Systems 41, part 1/4, edited by C.T. Leondes, Academic Press, San Diego, CA, 1991.

T. Dillon, and Niebur, D. (eds) "Neural Net Applications in Power Systems," To be published, CRL Publishing Ltd, Leics, UK, 1995.

R. Fischl and J. C. Chow, "Probabilistic Evaluation of Security Criteria in Power System Security Assessment," Pmt. of 1993 North American Power Symposium, Washington D.C., Oct. 11-12, 1993.

A J. Germond and D. Niebur, "Neural Network Applications in Power Systems," Invited Tutorial, J 1th PSCC Avignon, Butterworth, London, UK, 1993.

IEEE TF Report, "Survey of Applications of Artificial Neural Networks to Power Systems," Edited by Hiroyuki Mori, IEEE PES Task Force on Applications of Artificial Neural Networks to Power Systems, in preparation.

H Mori and S. Tsuzuki, "Artificial Neural Net Applications irr Power Systems in Japan," Proc of Workshop on Applications of Artificial Neural Network Methodology in Power Systems Engineering, pp. 13-17, Clemson, Smith Carolina, Oct. 1990.

H.H. Yan, R. Fischl and J-C Chow, "Indices for Evaluation of Neural Network Performance in Power System Security Assessment," Proc. of the Symposium on Intelligent System Application to Power Systems (ISAP), pp. 187-191, Montpellier, France, Sept. 1994.

STATIC SECURITY ASSESSMENT

Multi-Layer Perceptrons

M. Aggoune, M. A. El-Sharkawi, D.C. Park, M.J. Damborg, and R.J. Marks II, "Preliminary Results on Using Artificial Neural Networks for Security Assessment," IEEE Proc. of 1989 PICA, pp. 252-258, Seattle, Washington, U.S.A., May 1989.

M.E. Aggoune and S.V. Vadari, "Large Scale Power Systems Static Security Assessment Using Neural Networks," Proc. of NEURONET '90, pp. 10-12, Prague, Czechoslovakia, Sep. 1990.

ME Aggoune, LE. Atlas, D.A. Cohn, M.J. Damborg, M.A. El-Sharkawi and R.J. Marks 11, "Artificial Neural Networks for Power System Static Security Assessment," IEEE Proc. of 1989 ISCAS, pp. 490-494, Portland, Oregon, U.S.A., May 1989.

B.H. Chowdhury and B.M. Wilamowski, "Security Assessment Using Neural Computing," Proc. of ANNPS '91, pp. 54-58, Seattle, WA, July 1991.

M A. I l-Sharkawi, R.J Marks, M.J. Damborg, L.E. Atlas, D.A. Colm and M.E Aggoune, "Artificial Neural Networks as Operator Aid for On-Line Static

Security Assess ment of Power Systems", Proc. of 10th PSCC, pp. 895-901. Graz, Austria, Aug. 1990.

EPRI Report, "Power System Dynamic Security Analysis Using Artificial Intelligence S ystems, Phase I-Feasibility Evaluation", EPRI Project RP 3103-2, 1993

R. Fischl, M. Kam, J.-C. Chow and S. Ricciardi, "Screening Power System Contingency Using a Back Propagation Trained Multiperceptrons," IEEE Proc. of 1989 ISCAS, pp. 486-489, Portland, Oregon, U. S. A., May 1989.

S. Oh, R,]. Marks II, and M.A. El-Sharkawi, "Query Based Learning in a Multi-layered Perceptron," Proc. of 'ANNPS 91, pp. 72-75., Seattle, WA, July 1991.

Weerasooriya, S. and M.A. El-Sharkawi, "Use of Karhunen-Loève Expansion in Training Neural Networks for Static Security Assessment," Proc. of 'ANNPS '91, pp. 59-64, Seattle, WA, July 1991.

S. Weerasooriya and M. A El-Sharkawi, 'Towards *static security assessment* of large scale power systems using neural networks," IEE Proceedings< Generation, Transmission, and Distribution, vol Jissue 139/J, pp 64-70, January, 1992.

HH. Yan, J-C. Chow, M. Kam, C.R. Sepich and R. Fischl, "Design of a Binary Neural Network Security Classification in Power System Operation," IEEE Proc. of 1991 ISCAS, pp. 1121-1124. Singapore, June 1991.

H.H. Yan, J-C. Chow, M. Kam, R. Fischl and C.R. Sepich, "Hybrid Expert Systcnt/Neural Networks Hierarchical Architecture for Classifying Power System Contingencies," Proc. of 'ANNPS '91, pp. 76-82, Seattle, WA, July 1991.

J.J. Sanchez-Gasca, D.B. Klapper and J. Yoshizawa, "Back-Propagation as the Solution of Algebraic-Differential Equations for Artificial Neural Network Training," Proc. of 'ANNPS '91, pp. 242-246, Seattle, *WA*, July 1991.

S. Weerasooriya and M.A. El-Sharkawi, "Feature Selection for Static Assessment Using Neural Networks," IEEE Proc. of 1992 ISCAS, pp. 1693-1696, San Diego, California, U.S.A., May 1992.

Hopfield Nets

J-C. Chow, R. Fischl, M. Kam, H.H. Yan and S. Ricciardi, "An Improved Hopfield Model for Power System Contingency Classification," IEEE Proc. of 1990 ISCAS, pp. 292 S-2928, New Orleans, Louisiana, U.S. A., May 1990.

R. Fischl, M. Kam, J. C Chow, H. H. Yan, "Go the Design of Neural Networks for 1 Detecting the Limiting Contingencies in Power S ystem Operation," Power System Computation Conference, Graz, Austria, August 19-24, 1990, pp. 887-894.

M. Kam and R. Fischl, "Design of Asynchronous Binary Neural Using Linear Programming," Proc. of Workshop on Application. of Artificial Neural Network Methodology in Power S ystems Engineering, pp. 3 1-35, Clemson, South Carolina, Oct. 1990.

Y. Hayashi, S. Iwamoto, S. Matsuda and Y. Akimoto, "Introduction of Neural Network Theory In Newton-Raphson Load Flow," Proc. of Third Symposium on Expert *Systems* Application to Power Systems, pp. 343-350, Tokyo, Japan, Apr. 1991.

II Mori, "Quadratic Load Flow Calculation in Electric Power Systems Using a Hopfield Model," Proc. of ICANN '92, pp. 1667-1670, Brighton, U. K., Sep. 1992.

HMori, N. Kitani and S. Tsuzuki, "Optimal Power Flow calculation Using the Hopfield Net," Proc. of Third Symposium no Expert S ystems Application to Power Systems, pp. 328-335, Tokyo, Japan, Ape. 1991.

R.J. Thomas, E Sakk, K. Hashemi, B.Y. Ku and H-D. Chiang, "On-Line Security Screening Using and Artificial Neural Network," IEEE Proc. of 1990 ISCAS, pp. 2921-2924, New Orleans, Louisiana, U. S. A., May 1990.

II. H. Yan and R. Fischl, "Power System Security Assessment Using a Hybrid Expert System/Neural Networks Architecture," IEEE Pmt. of 1992 ISCAS, pp. 1713-1716, San Diego, California, U.S.A., May 1992.

Kohonen Nets

Cornu, T., Ienne, P., Niebur, D and Viredaz, M., "A S ystolic Accelerator foc Power System Security Assessment.," Proc. of ISAP '95, pp. 431-438, Montpellier, France, September 94.

M.A. El-Sharkawi and R Atteri, "Static Security Assessment of Power System Using the Kohonen Neural Network," ANNPS93', Tokyo, Japan, pp. 373.377, April 1993.

D. Niebur and A.J. Germond, "Unsupervised Neural Net Classification of Power System Static Security States," Electrical Power and Energy Systems, Vol 14, No. 2/3, pp. 233-242 April/June 1992.

D. Niebur, A. J Germond, "Power System Static Security Assessment Using the Kohonen Neural Network Classifier, " Power Industry Computer Application Conference, Baltimore, MD, May 1991, pp. 270-277, also in IEEE 1 ransactions on Power Systems, Vnf 7, No. 2, pp.865-872, May 1992.

Other ANNs

M. A. El Sharkawi and Steven S. Huang, "Ancillary Techniques for Neural Network Applications," IEEE World Congress on Computational Intelligence; ICNN '94, Orlando, *Florida.* June 28- July 2, 1994.

M.A. El-Sharkawi and Steven S. Huang, "Application of Genetic-Based Neural Networks to Power System Static Security Assessment," International Conference on Intelligent System Application to Power Systems, Montpellier, France, September s-9. 1994.

S.-Y. Oh, "A Pattern Recognition and Associative Memory Approach to Power System Security Assessment, " IEEE Transactions on Systems, Man and Cybernetics, Vol SMC16, Nn. 1, Jan/Feb 1986, pp. 62.

Ranaweera, D. K. and Karady, G., "Power System Security Analysis Using Radial Basis Function Neural Network," Procs. of the 4th Symposium on Expert System Application to Power Systems, Melbourne, 1993, pp. 272-274.

I). J. Sobajic, Y. H. Pan. W Njo and J.L. Dolce, "Real-Time Security Monitoring of Electric Power S ystems Using Paral IcI Associative Memorie s," IEEE Proc of 199(1 ISCAS, pp. 2929-2932, New Orleans, Louisiana, U. S. A., May 1990

DYNAMIC SECURITY ASSESSMENT

Multi-l *ayer Perceptrons*

M.E. Aggoune, M.J. Damborg, M.A. El-Sharkawi, R.J. Marks 11, arrd L.E. Atlas, "Dynamic and Static Security Assessment of Power Systems Using Artificial Neural Networks," Proc. of Workshop on Applications of Artificial Neural Network Methodology in Power Systems Engineering, pp. 26-30, Clemson, South Carolina, Oct. 1990.

C-R. Chen, and Y-Y. Hsu, "Synchronous Machine S[eady-State Stability Analysis Using an Artificial Neural Network," IEEE PES 1990 Summer Meeting, Paper No. 90 SM 430-9EC, Minneapolis, Minnesota, U. S. A., July 1990.

Djukanovic, M., Sobajic, 1). J. and Pan, Y.H., "Neural net based calculation of voltage dips at maximum angular swing in direct transient stability analysis", Electric Power and Energy Systems, Vol. 14, no.. 5, pp. 341-350, October 1992.

Djukanovic, M., Sobajic, D J. and Pan, Y. H., "Neural net based determination of generator shedding requirements in electric power systems", IEE Proc. *C - Vol.* 139, No 5, pp 2S5.262, September 1992.

M. A. El-Sharkawi, R.J. Marks II, M.E. Aggoune, D.C. Park, M.J. Damborg and I E. Atlas, "Dynamic Security Assessment of Power Systems using Bark J Error Propagation Artificial Neural Networks," Second Symposium on Expert S ystem Application In Power S ystems, Seattle, WA, 1989.

J.N. Fidalgo, Peças Lopes, J. A., Miranda, V., and Almeida, J., "Fast Assessment of Transient Stability Margins by a Neural Network Approach", Pmt. of the 11th PSCC, Avignon, August 1993.

Hui, K D.. and Short, M. J., "A Neural Networks Approach to Voltage Security Monitoring", First International Forum on Applications of Neural Networks 10 Power Systems, Seattle, July 1991, pp. 89-93.

A.B.R Kumar, A. Ipakchi, V. Brandwajn, M.A. El-Sharkawi and G. Cauley, "Neural Networks for Dynamic Security Assessment of Large-Scale Power *Systems,*" Proc. of 'ANNPS '91, pp. 65.71, Seattle, WA, July 1991.

II. Mori, "An Artificial Neural-Net Based Method for Estimating Power System 1 Dynamic Stability Index," Proc. of 'ANNPS '91, pp. 127-133, Seattle, WA, July 1991.

D. Novosel and R.L. King, "Identification of Power System Emergency Actions Using Neural Networks," Proc of 'ANNPS '91, pp. 205-209, Seattle, WA, July 1991.

M. A. El-Sharkawi and Steve.n S. Huang, "Query-Based Learning Neural Network Approach to Power System Dynamic Security Assessment," International Symposium on Nonlinear Theory and its Applications, Waikiki, Hawaii, December 5-10, 1993.

D.J. Sobajic and Y-H. Pao, "Artificial Neural-Ncl Based Dynamic Security Assessment for Electric Power Systems," IEEE Trans. on Power Systems, Vol 4, No. 1, pp. 220-4, Feb. 1989

R. Thomas, "Experiences with Security Classification Using an Artificial Feed Forward Neural Network," Proc. of Workshop on Applications of Artificial Neural Network Methodology in Power S ystems Engineering, pp. 129-140, Clemson, South Carolina, Oct. 1990.

V. Vittal and J. Davidson, "Application of ANN to Analyze the Security of a Transient-Voltage Limited Power Network," Proc. of Workshop on Applicat ions of Arti ficial Neural Network Methodolog y in Power S ystems Engineering, pp. 36-41, Clemson, South Carolina, Oct. 1990.

S. Weerasooriya and M. A. El-Sharkawi, "Dynamic Security Assessment of Power Systems Using Neural Networks," International Conference cm Expert System Applications for the Electric Power Industry, Phoenix, Arizona, December 8-10.1993.

Q. Zhou, J. Davidson and A. A Fouad, "Application of Artificial Neural Networks in Power System Security and Vulnerability Assessment," IEEE PES 1993 Winter Meeting, Paper No. 93 WM 183-4-PWRS, Columbus, Ohio, U.S.A., Jan. 1993.

Kohonen Nets

H. Mini, Y. Tamaru and S. Tsuzuki, "An Artificial Neural-Net Based Technique for Power System Dynamic Stability with the Kohonen Model," IEEE Proc. of 1991 PICA, pp. 293-301, Baltimore, Maryland May, 1991.

H. Mori and Y. Tamaru, "An Artificial Neural-Net Based Approach to Monitoring Power System Voltage Stability," Pmt. of Bulk Power System Voltage Phenomena 11, Voltage Stability and Security, Deep Creek Lake, MA, U.S. A., Aug. 1991.

H. Mori and Y. Tamaru, "J lybrid Artificial Neural Network for Voltage Instability in Electric Power Systems," Proc. of IEEE International Conference m SMC, pp. 151-156, Illinois, U.S.A., Oct 1992.

H. Mori, H. Miyamoto and S. Tsuzuki, "Estimation of a Voltage Stability Index with a Kohonen Neural Net work, " Proc. of ICARCV '92, Paper No. INV-11.5, Singapore, Sep. 1992.

Other ANNs

H. Asadi, A. Tan, M. Etezadi-Amoli, D. Egbert and M.S. Fadali, "Applications of ARTMAP Neural Network to Power System Stability Studies," Proc. of IEEE International Conference on S ystems, Man, C, pp. 108 O- 10S5, Chicago, U. S. A., Oct. 1992.

Miranda, V., Fidalgo, J. N., Peças Lopes, J. A., and Almeida, J., "Real Time Preventive Actions for Transient Stability Enhancement with a Hybrid Neural Network - Optimization Approach," IEEE Summer Meeting, Sarr Francisco, July 1994, no. 94 SM 517-3 PWRS

C.K. Pang, F.S. Prabhakara, A.H. El-Abiad, and A.J. Koivo, "Security Evaluation in Power S ystems Using Pattern Recognition," IEEE Trans. on Power, Apparatus and Systems, vol. PAS-93 No. 2, pp. 969-976, May/June 74.

Y-H. Pao rural D.J. Sobajic, "Combined Use of Unsupervised arrd Supervised Learning for Dynamic Security Assessment," IEEE Proc. of 1991 PICA, pp. 278-284, Baltimore, Maryland, U. S. A., May. 1991.

D., Sobajic, Y.H. Pao, and J. Dolce, "~!-line monitoring and diagnosis of power system operating conditions using artificial neural networks," Proc of the 1989 ISCAS, vol. 3, pp ?243-2?46, Portland, OR, May, 1989.

S.V. Vadari and S S. Venkata, "A Hybrid Neural N@wmk/Artificial Intelligence Approach for Voltage Stability Enhancement," Proc. of 'ANNPS '91, pp. 154-160, Seattle, WA, July 1991.

Wehenkel, L., Van Cutsem, T. and Pavella, M., Heilbronn, B. and Pruvot, P., "Machine Learning, Neural Networks and Statistical Pattern Recognition for Voltage Security: A Comparative Study," Proc. ISAP'94, Montpellier, France, September 1994, pp. 521-528.